

**IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF DELAWARE**

RYANAIR DAC,

Plaintiff,

v.

C.A. No. 20-01191-WCB

BOOKING HOLDINGS INC.,
BOOKING.COM B.V., KAYAK
SOFTWARE CORPORATION,
PRICELINE.COM LLC, and AGODA
COMPANY PTE. LTD,

Defendants.

**BRIEF OF DEFENDANT BOOKING.COM IN SUPPORT OF
MOTION FOR JUDGMENT AS A MATTER OF LAW**

OF COUNSEL:

John H. Hemann
Kathleen Hartnett
Kristine Forderer
Alexander J. Kasner
Jessie Simpson LaGoy
Hannah Pollack
Zoë Helstrom
COOLEY LLP
3 Embarcadero Center, 20th Fl.
San Francisco, CA 94111
(415) 693-2200
jhemann@cooley.com
khartnett@cooley.com
kforderer@cooley.com
akasner@cooley.com
jsimpsonlagoy@cooley.com
hpollack@cooley.com
zhelstrom@cooley.com

Jeffrey L. Moyer (#3309)
Alexandra M. Ewing (#6407)
Richards, Layton & Finger, P.A.
One Rodney Square
920 N. King Street
Wilmington, DE 19801
(302) 651-7700
moyer@rlf.com
ewing@rlf.com

*Attorneys for Defendant/Counterclaim
Plaintiff Booking.com B.V.*

Dated: July 17, 2024

TABLE OF CONTENTS

	<u>PAGE</u>
I. INTRODUCTION	1
II. LEGAL STANDARD.....	1
III. BOOKING.COM IS ENTITLED TO JUDGMENT AS A MATTER OF LAW ON ALL CLAIMS BECAUSE NO REASONABLE JURY COULD CONCLUDE THAT RYANAIR HAS SHOWN \$5,000 OR MORE OF LOSS IN A ONE-YEAR PERIOD ATTRIBUTABLE TO BOOKING.COM.	2
A. Claimed “Losses” From Investigating And Responding To Offenses.	3
B. Claimed “Losses” Attributable To Customer Verification Procedures.	6
C. Claimed “Losses” From The “Monex” Incident.....	10
IV. BOOKING IS ENTITLED TO JUDGMENT AS A MATTER OF LAW ON ALL CLAIMS BECAUSE NO REASONABLE JURY COULD CONCLUDE THAT RYANAIR HAS ESTABLISHED KEY ELEMENTS OF ITS CFAA CLAIMS.	12
A. Count IV (18 U.S.C. § 1030(a)(5)(B)-(C)) (Access Without Authorization).....	12
B. Count II (18 U.S.C. § 1030(a)(4)) (Fraud).....	14
C. Count V (18 U.S.C. § 1030(b)) (Conspiracy).....	15
V. DEFENDANTS ARE ENTITLED TO JUDGMENT AS A MATTER OF LAW BECAUSE RYANAIR HAS FAILED TO ESTABLISH A FACTUAL BASIS FOR THE EXTRATERRITORIAL APPLICATION OF THE CFAA.	16
VI. CONCLUSION.....	20

TABLE OF AUTHORITIES

	Page(s)
CASES	
<i>Abitron Austria GmbH v. Hetronic Int’l, Inc.</i> , 600 U.S. 412 (2023).....	16, 18, 20
<i>Condux Int’l, Inc. v. Haugum</i> , 2008 WL 5244818 (D. Minn. Dec. 15, 2008).....	7
<i>Czech v. Wall St. on Demand, Inc.</i> , 674 F. Supp. 2d 1102 (D. Minn. 2009).....	8
<i>Fidlar Techs. v. LPS Real Est. Data Sols., Inc.</i> , 810 F.3d 1075 (7th Cir. 2016)	14, 15
<i>Liqwd, Inc. v. L’Oreal USA, Inc.</i> , No. 17-14-JFB-SRF, D.I. 1064 (D. Del. Aug. 15, 2019).....	1, 2
<i>Pulte Homes, Inc. v. Laborers’ Intern. Union of North America</i> , 648 F.3d 295 (6th Cir. 2011)	7, 8
<i>QVC, Inc. v. Resultly, LLC</i> , 159 F. Supp. 3d 576 (E.D. Pa. 2016)	14
<i>United States v. Carlson</i> , 209 Fed. App’x 181 (3d Cir. 2006).....	8
<i>United States v. Nosal</i> , 676 F.3d 854 (9th Cir. 2012)	19
<i>Van Buren v. United States</i> , 593 U.S. 374 (2021).....	7
<i>Walter v. Holiday Inns, Inc.</i> , 985 F.2d 1232 (3d Cir. 1993).....	1
<i>Worldspan, L.P. v. Orbitz, LLC</i> , 2006 WL 1069128 (N.D. Ill. Apr. 19, 2006)	7
STATUTES & RULES	
Computer Fraud and Abuse Act, 18 U.S.C. § 1030.....	<i>passim</i>
Lanham Act.....	18

OTHER AUTHORITIES

https://csrc.nist.gov/glossary/term/data_integrity7

I. INTRODUCTION

Defendant Booking.com B.V. (“Booking.com”) hereby moves pursuant to Federal Rule of Civil Procedure 50(a)(1) for judgment as a matter of law on all of Plaintiff Ryanair DAC (“Ryanair”)’s remaining claims in this action. Ryanair has been fully heard, having presented its affirmative evidence and rested its case. There are several grounds warranting judgment as a matter of law in favor of Booking.com on Ryanair’s claims.

First, Ryanair has failed to show Loss under the Computer Fraud and Abuse Act (“CFAA”) attributable to Booking.com in the amount of \$5,000 or more in a one-year period, as required to maintain a civil action under the CFAA. Second, Ryanair has otherwise failed to show essential elements of its CFAA claims, including: unauthorized access with the requisite intent, loss, damage, fraud, or conspiracy. Third, Ryanair has failed to establish a factual basis for the extraterritorial application of the CFAA in this case.

Because there is not a legally sufficient evidentiary basis for a jury to find for Ryanair on its CFAA claims, judgment as a matter law should be entered for Booking.com.

II. LEGAL STANDARD

Judgment as a matter of law is appropriate after the moving party is fully heard and where the Court “finds that a reasonable jury would not have a legally sufficient evidentiary basis” to find for the nonmoving party. Fed. R. Civ. P. 50(a)(1); *see Walter v. Holiday Inns, Inc.*, 985 F.2d 1232, 1238 (3d Cir. 1993). “The question is not whether there is literally no evidence supporting the party against whom the motion is directed but whether there is evidence upon which the jury could properly find a verdict for that party.” *Liqwd, Inc. v. L’Oreal USA, Inc.*, No. 17-14-JFB-SRF, D.I. 1064 at 1-2 (D. Del. Aug. 15, 2019). A judgment as a matter of law is properly “granted where the record is critically deficient of the minimum quantum of evidence necessary to support

a jury verdict” for the nonmoving party. *Id.* (citing *Eshelman v. Agere Sys. Inc.*, 554 F.3d 426, 433 (3d Cir. 2009)) (internal quotation marks omitted).

III. BOOKING.COM IS ENTITLED TO JUDGMENT AS A MATTER OF LAW ON ALL CLAIMS BECAUSE NO REASONABLE JURY COULD CONCLUDE THAT RYANAIR HAS SHOWN \$5,000 OR MORE OF LOSS IN A ONE-YEAR PERIOD ATTRIBUTABLE TO BOOKING.COM.

To sustain a civil action under the CFAA, Ryanair must show that it has “suffer[ed] damage or loss by reason of a violation” of the CFAA. D.I. 399 (“MSJ Opinion”) at 21 (quoting 18 U.S.C. § 1030(g)). Five potential ways of showing such “damage or loss” are set forth in Section 1030(c)(4)(A)(i), but the only one relevant here requires Ryanair to prove that Booking.com’s alleged violation of the CFAA caused Ryanair “loss to 1 or more persons during any 1-year period . . . aggregating at least \$5,000 in value[.]” D.I. 399 at 21 (quoting 18 U.S.C. § 1030(c)(4)(A)(i)(I)). “Loss” means “any reasonable cost to any victim, including the cost of responding to an offense, conducting a damage assessment, and restoring the data, program, system, or information to its condition prior to the offense, and any revenue lost, cost incurred, or other consequential damages incurred because of interruption of service.” 18 U.S.C. § 1030(e)(1).

As Ryanair explained in its summary judgment motion, its claimed one-year CFAA loss period for Booking.com runs “from March 1, 2022, to February 28, 2023 (the ‘Booking Period’).” D.I. 348 at 9 n.2, 14-15. The MSJ Opinion assessed two general categories of “loss” claimed by Ryanair to meet the \$5,000 threshold: (1) “[l]osses from investigating and responding to offenses,” D.I. 399 at 23-30, and (2) “[l]osses attributable to customer verification procedures,” *id.* at 31-32. Although the Court determined that certain of Ryanair’s claimed “losses” in these categories were unavailable as a matter of law, *see, e.g., id.* at 28 (barring costs of certain prophylactic measures), it also determined that some of Ryanair’s claimed losses were theoretically available if supported

by Ryanair’s evidence at trial. *See id.* at 28-32.¹ It also addressed what Ryanair would need to show regarding the so-called “Monex attack.” *Id.* at 30. Ryanair has now presented its case, and no reasonable jury could conclude that it has shown \$5,000 or more of loss in a one-year period attributable to Booking.com for *any* of these categories, separately or cumulatively.

Before detailing below how Ryanair has failed to substantiate its loss claims in every category addressed by the MSJ Opinion, Booking.com makes one initial, overarching point with respect to “loss.” Ryanair seeks to attribute—across the board—2.8% of all of its claimed OTA costs to Booking.com. However, Ryanair’s evidence at trial does not support this calculation or approach. Ryanair relied on data from Booking.com to arrive at the number of Booking.com bookings during the claimed loss period. However, Ryanair failed to introduce at trial reliable evidence to establish the number of total Ryanair OTA bookings during the period, from which any percentage attributed to Booking.com could be derived. *See* 7/15/24 Trial Tr. at 144-46 (Hurley) (claiming that numbers provided to witness by counsel “look right” and “sound right,” but not providing any substantiation, and otherwise providing unclear at best math on the stand).

A. Claimed “Losses” From Investigating And Responding To Offenses.²

Shield Hosting Costs. Under the MSJ Opinion, “[t]o the extent that the facts at trial show that Shield prevents unauthorized bookings at the payment page after account creation, any portion

¹ The MSJ Opinion, while excluding certain of Ryanair’s claimed losses, rejected Defendants’ argument “that a qualifying ‘loss’ must result from technological harm and that Ryanair has not shown any such harm.” D.I. 399 at 23 (citing D.I. 335 at 27). Instead, the Court ruled that “term ‘loss’ is best understood to include the cost of an investigation following a CFAA violation, even in instances in which the violation has not resulted in actual impairment of the protected computer or loss of data.” D.I. 399 at 26. Booking.com preserves its challenge to this ruling; under the CFAA, “loss” must flow from responding to an actual “technological harm.” *See* D.I. 335 at 27-28 (Defendants’ opening summary judgment brief); D.I. 378 at 10-13 (Defendants’ summary judgment reply). However, as set forth in this brief, even under the Court’s framework, Ryanair has failed to attribute \$5,000 or more of loss in a one-year period to Booking.com.

² This section addresses Ryanair’s claimed losses discussed in the MSJ Opinion at pages 28-30, with subheadings to track those in the Court’s opinion, with the exception that Shield Software

of those costs allocable to each defendant.” D.I. 399 at 28. Yet the evidence at trial shows that Shield has only a single endpoint on the myRyanair portion of the Ryanair website prior to a payment having successfully been made. 7/16/24 Trial Tr. at 350-51 (Stocki). Ryanair referred to this as “Shield Lite” and testified that it takes less than one second to perform its analysis. *See id.* at 351. Shield then analyzes bookings *post*-payment with a more complex version of the algorithm that takes 5-20 minutes. *See id.* Plainly an endpoint after a payment has been made is not a means of “prevent[ing] unauthorized bookings.” D.I. 399 at 288. In any event, Ryanair has failed to reliably attribute any of its pre-payment myRyanair “Shield Lite” costs to Booking.com, let alone in an amount of \$5,000 or more in a one-year period. Indeed, Ryanair introduced no evidence of the hosting costs for approximately half of the period in question (March 1, 2022 to February 28, 2023). Even applying Ryanair’s flawed methodology of assuming that one endpoint accounts for 50% of its Shield costs, and then applying its unsubstantiated 2.8% attribution of all OTA costs to Booking.com, Ryanair did not present evidence establishing anywhere near \$5,000 of loss attributable to Booking.com. 7/16/24 Trial Tr. at 340, 351 (Stocki).

Business Intelligence Employees. Under the MSJ Opinion, “contingent on proving that bot activity damages the integrity of its data, Ryanair may include the costs entailed in its business intelligence employees’ activities relating to remedying the harms of bot activity.” D.I. 399 at 29.³ At trial, Ryanair put in no evidence about any business intelligence employee-related costs at all.

Cloudfront and Amazon AWS Firewall. Under the MSJ Opinion, Ryanair may “include the costs of Cloudfront and AWS-WAF to the extent that Ryanair can attribute those costs to

Development and New Relic costs are not discussed, as the Court determined in its MSJ Opinion that Ryanair may not include as a matter of law. *See* D.I. 399 at 29.

³ Although the MSJ Opinion did not expressly state in this portion that Ryanair could only allocate a portion of such costs to Booking.com, the rest of its opinion makes clear that any overall costs entailed in remedying such harms would have to be allocated to Booking.com.

denying unauthorized booking requests by the defendants,” and “[b]ecause both Cloudfront and AWS-WAF have multiple purposes, Ryanair must be able to attribute costs specifically to unauthorized bot activity that violates the CFAA.” D.I. 399 at 30.

Ryanair’s evidence at trial has shown *no* Cloudfront costs related to denying allegedly unauthorized bookings by Booking.com. *See* 7/16/24 Trial Tr. at 362 (Stocki). To the contrary, Ryanair’s evidence has shown that Cloudfront, though it also sends certain information to Shield, is primarily intended to render the images that appear on Ryanair’s website and mobile app quickly and, most critically, that Ryanair would use Cloudfront for that purpose, even if it were not sending information to Shield. *Id.* at 362-64. Ryanair did not attempt to apportion any part of its claimed Cloudfront costs to Cloudfront’s interaction with Shield, or to any post myRyanair blocking activity, contrary to the Court’s direction in the Order.

And, with respect to AWS-WAF, Ryanair has put in no loss evidence whatsoever.

Navitaire and my Ryanair. Under the MSJ Opinion, Ryanair can claim costs related to Navitaire and myRyanair as “loss” if “the facts developed at trial show that the bot traffic attributable to the defendants has materially increased the cost of Ryanair’s server infrastructure.” *Id.* at 30. Ryanair’s evidence at trial has made *no* showing that any bot traffic allegedly attributable to Booking.com “has materially increased the cost of Ryanair’s server infrastructure.”

With respect to Navitaire, the evidence shows that, at most, Booking.com-related traffic is 0.6% of Navitaire activity during the Loss Period, making it *de minimis*, not “material.” *See* 7/15/24 Trial Tr. at 146:7-19, 144:4-8 (Hurley). Further, the Navitaire contract in evidence contains mandatory minimum number of bookings and Ryanair has not introduced evidence that any Booking.com booking was above the minimum required for the period, for which Ryanair would have had to pay regardless. DTX-202.

With respect to myRyanair, Ryanair introduced no evidence of loss, at all. This includes its witness's testimony that 60% of myRyanair accounts are attributable to OTAs, as Ryanair responded to Booking.com's objection by disclaiming that it was using this testimony to establish loss. 7/16/24 Trial Tr. at 301-302 (Hurley).

B. Claimed "Losses" Attributable To Customer Verification Procedures.⁴

In addition to Ryanair's claimed losses from "investigating and responding to offenses," the Court separately determined that there were factual issues for trial with respect to Ryanair's "verification" procedures for OTA customers, namely: (1) "whether the OTA bookings affect the integrity of Ryanair's data" because "such bookings input information into Ryanair's database that never should have been there in the first place"; (2) "whether Ryanair's verification measures are directed at data integrity or were simply a business practice designed to discourage the use of OTAs"; and (3) "whether the OTAs' customer details and payment methods are in fact 'fake.'" D.I. 399 at 32. Ryanair's evidence has conclusively shown a failure to meet these requirements.

At the outset, Booking.com respectfully disagrees with the Court's statement in its MSJ Opinion that "the question whether the OTA bookings affect the integrity of Ryanair's data turns on whether the bookings were unauthorized," and that "[i]f Ryanair is correct in its theory of the case, the unauthorized bookings affect Ryanair's data integrity because such bookings input information into Ryanair's database that never should have been there in the first place." D.I. 399 at 32. This conception of "data integrity"⁵ is against the weight of authority, as numerous courts

⁴ This section addresses Ryanair's claimed losses discussed at pages 31-32 of the MSJ Opinion.

⁵ The National Institute of Standards & Technology's ("NIST's") definitions of "data integrity" correspond to this point. See https://csrc.nist.gov/glossary/term/data_integrity (listing NIST definitions of "data integrity," such as "[t]he property that data has not been altered in an unauthorized manner," and "[a] property whereby data has not been altered in an unauthorized manner since it was created, transmitted, or stored"). As the Supreme Court has explained in interpreting the CFAA, "[w]hen interpreting statutes, courts take note of terms that carry 'technical meaning[s].'" *Van Buren v. United States*, 593 U.S. 374, 388–89 (2021).

have held that “data integrity” in the context of the CFAA does not mean additional, unwanted data (as Ryanair claims), but rather “some *diminution* in the completeness or useability of data or information on a computer system.” *Worldspan, L.P. v. Orbitz, LLC*, 2006 WL 1069128, at *5 (N.D. Ill. Apr. 19, 2006) (quoting *Resdev, LLC v. Lot Builders Ass’n*, 2005 WL 1924743, at *5 n.3 (M.D. Fla. Aug. 10, 2005)) (emphasis added); *Condux Int’l, Inc. v. Haugum*, 2008 WL 5244818, at *8 (D. Minn. Dec. 15, 2008) (diminution of data integrity entails “alteration of or diminution to the integrity . . . of the computer data itself”).

The data of which Ryanair complains (working e-mail addresses and valid virtual credit cards, in a number commensurate with the number of passengers), did nothing to diminish Ryanair’s access to or completeness of existing data. The working e-mails Ryanair received, for instance, were not a “blitz” designed to “wreak[] . . . havoc” by “overloading [a] system” and “stall[ing] normal business operations because [] employees could not access business-related e-mails or send e-mails to customers and vendors.” *Pulte Homes, Inc. v. Laborers’ Intern. Union of North America*, 648 F.3d 295, 299 (6th Cir. 2011). Indeed, the Sixth Circuit made precisely this distinction in *Pulte Homes*: while a volume-based e-mail attack which diminishes ability to access existing data is “damage,” the mere sending of sending unwanted data itself does not constitute damage or impairment to data (*id.* at 301-302, contrasting *Czech v. Wall St. on Demand, Inc.*, 674 F. Supp. 2d 1102, 1115-16 (D. Minn. 2009), which held that a defendant sending unwanted cell messages to plaintiff, which “consum[ed] limited resources,” is not CFAA “damage”); *see also United States v. Carlson*, 209 Fed. App’x 181, 184-85 (3d Cir. 2006) (sending of “thousands of e-mails” is CFAA damage to the extent it “impair[ed] the user’s ability to access his other ‘good emails’”). At trial, Ryanair has shown no “diminution” in the completeness or useability of data on the Ryanair system; at most, it has shown that it received unwanted data from OTAs, including

Booking.com. Accordingly, judgment as a matter of law must be entered against Ryanair on its “data integrity” theory of loss.

Even under the Court’s conception of “loss” based on impaired data integrity, however, Ryanair has failed to make the required showing at trial with respect to its verification processes—i.e., that it receives “fake” customer details and payment methods regarding Booking.com customers, and that its verification processes are directed at data integrity rather than “simply a business practice designed to discourage the use of OTAs.” D.I. 399 at 32. Ryanair’s own case has shown that Ryanair receives usable data—real, functioning email addresses and real, functioning credit card numbers—when Ryanair flights are booked via Booking.com. 7/15/24 Trial Tr. at 219:22-24 (Hurley); 7/16/24 Trial Tr. at 398-402 (Lopata). Indeed, Ryanair has conceded at trial that other than with respect to OTAs, it does not consider data “fake” or “lacking integrity” just because a passenger’s name does not correspond to the email address or credit card provided, so long as there is a working email address or credit card used. 7/15/24 Trial Tr. at 212:8-21 (Hurley). Thus, Ryanair’s verification process is not directed at data integrity, but at “owning” the customer. Moreover, Ryanair has failed to attribute any claimed “data integrity” issues to Booking.com—as opposed to OTAs generally—and its own evidence establishes that Ryanair *can* communicate with customers who book Ryanair flights through Booking.com (7/15/24 Trial Tr. at 214:9-12 (Hurley); 7/16/24 Trial Tr. at 398-402 (Lopata));⁶ that Ryanair has been paid for Booking.com bookings (7/16/24 Trial Tr. at 291-92 (Hurley); *id.* at 401-402 (Lopata)); and that there is no evidence that Booking.com customers do not receive refunds (7/15/24 Trial Tr. at 217:8-15 (Hurley)). Finally, the evidence presented in Ryanair’s case

⁶ Hurley claimed to have made two test bookings in the last two weeks (7/15/24 Trial Tr. at 225-26), but failed to provide any substantiating evidence for these bookings and this evidence is otherwise contrary to discovery and evidence otherwise presented by Ryanair at trial.

established that Ryanair is aware that *approved* travel agent partners do *not* send Ryanair the passenger's own email address. *See* 7/16/24 Trial Tr. at 414-17 (Lopata). That Ryanair accepts such email addresses from other travel agents further undermines any claim of impaired data.

Further, Ryanair has not demonstrated proper attribution of the alleged costs themselves—for online verification and customer service—to Booking.com. In particular, the online verification costs are calculated by multiplying the number of OTA-related verifications times \$0.59 (Ryanair's cost of using GetID for the verification). 7/15/24 Trial Tr. at 166:11-168:33 (Hurley). But this is not a true cost to Ryanair, because it is passed in full to the customer. *See, e.g.,* DTX-262. As to customer service, Ryanair has calculated this cost by multiplying the number of OTA-related customer service inquiries times the cost of the salaries of the customer service agents. 7/15/24 Trial Tr. at 170:13-23 (Hurley). However, Mr. Hurley testified that this methodology does not account for the subject matter of the inquiry (and whether it relates to any alleged data integrity) or the fact that a chatbot can verify an email address very quickly. 7/16/24 Trial Tr. at 277:14-278:4, 279:23-280:11 (Hurley). And as to both, each of which track customer PNR codes (*id.*), Mr. Hurley could offer no explanation as to why Ryanair could not provide the *actual number* of verifications and customer service inquiries that Booking.com customers made. *Id.* at 286:3-287:9.⁷

In short, that Ryanair wants more information from passengers who book through OTAs to “own” them is not a “data integrity” issue regarding the real information it receives in conjunction with Booking.com bookings.

⁷ As with Business Intelligence Employees, *see supra*, Ryanair has put in no evidence at trial regarding Digital Employee-related costs regarding verifications or otherwise.

C. Claimed “Losses” From The “Monex” Incident.⁸

In its MSJ Opinion, the Court concluded that “whether a portion of the Monex attack can be attributed to the defendants and whether the Monex attack damaged Ryanair’s systems are factual questions that are not suitable for resolution on summary judgment.” D.I. 399 at 30. Ryanair’s evidence is now in, and it has wholly failed to show that the Monex “attack” damaged its systems or that this incident can be attributed to Booking.com in any respect (let alone a material one). To the contrary, Ryanair’s trial evidence makes clear that Ryanair has failed to show—other than through speculation—that Booking.com (or Etraveli) perpetrated the Monex incident or caused any harm to Ryanair based on that incident. Judgment as a matter of law should be granted to Booking.com based on Ryanair’s claimed theory of Monex-related “loss.”

Prior to trial, Ryanair asserted the following potential “loss” related to Monex: “the inability to process certain credit cards,” “a lack of currency exchange services,” “additional employee time required to respond to the attack,” “Monex being unable to feed data to Shield,” and “increased traffic to their servers.” D.I. 343, Hemann Decl. Ex. 26. It also noted that that “Ryanair is losing revenue not being able to offer its currency conversion services to its passengers.” *Id.* Then, on the eve of trial, Ryanair claimed it would show at trial that it “lost revenues and lost profits due to the inability for customers to purchase flights from Ryanair during periods when the website was impaired or interrupted.” D.I. 407 at 20. At trial, however, Ryanair showed none of this. To begin, it wholly failed to show that Booking.com (or Etraveli) was

⁸ Booking.com preserves its challenge to the inclusion of the “Monex attack” at trial, for the reasons stated in its Motion *in Limine* No. 3 and its brief regarding Monex (D.I. 435). Additionally, as explained in Booking.com’s Monex brief, Ryanair should not be able to claim “loss” from the Monex incident because it was not properly disclosed and is not within Ryanair’s disclosed one-year loss period. D.I. 435 at 9 n.7. Moreover, Ryanair also cannot invoke the October 2023 Monex incident as alleged support for showing “loss” or “damage” under 18 U.S.C. § 1030(a)(5)(B) and (C), but then rely on conduct from March 2022 through February 28, 2023 to show \$5,000 or more of loss in a one-year period under Section 1030(g). D.I. 435 at 9.

responsible for all or part of the Monex incident, which, if anything, appears to have occurred as a result of the conduct of some unknown party. 7/16/24 Trial Tr. at 243-55 (Hurley). Indeed, Ryanair’s own witness stated that a similarly situated booking to Booking.com’s “could have been an innocent party” (7/16/24 Trial Tr. at 246:09 (Hurley)), and that the Monex incident was likely the work of one actor (*id.* at 246), whereas the one Booking.com booking presented at trial is connected, at most, to a small fraction of Ryanair’s claimed “errors” that day. But beyond the lack of any credible evidence connecting Booking.com to the Monex incident, Ryanair has shown no “loss” related to Monex that could be attributable to Ryanair. At trial, Ryanair’s claimed harm was reduced to \$13,000⁹ of chargebacks by MasterCard for all of October 2023 (none of which can be attributed to a Booking.com booking), and two hours of sporadically inoperable currency conversion services, during which time Mr. Hurley testified Ryanair flights could still be booked. 7/16/24 Trial Tr. at 258-61. Even if this \$13,000 could be apportioned according to the single booking with a Booking.com PNR code, it would be vastly less than \$5,000. In short, no reasonable jury could find *any* loss attributable to Booking.com based on the Monex “evidence.”

The MSJ Opinion provided Ryanair with a roadmap to proving at trial \$5,000 or more of loss attributable to Booking.com. Ryanair has wholly failed to do so in a way that could be accepted by a reasonable jury, as its “loss” claims are either unsupported by evidence, or relate to OTAs generally without any supported apportionment to Booking.com. Accordingly, Booking.com is entitled to judgment as a matter of law on all of Ryanair’s CFAA claims.

⁹ Originally, Mr. Hurley testified that Booking.com was responsible for a portion of a \$35,000 MasterCard chargeback for September 2023 that Mr. Hurley alleges was related to the Monex incident, but he then conceded that these charges could not be connected to any Booking.com PNR codes. 7/15/24 Trial Tr. at 185:5-186:10 (Hurley); 7/16/24 Trial Tr. at 262-63 (Hurley).

IV. BOOKING IS ENTITLED TO JUDGMENT AS A MATTER OF LAW ON ALL CLAIMS BECAUSE NO REASONABLE JURY COULD CONCLUDE THAT RYANAIR HAS ESTABLISHED KEY ELEMENTS OF ITS CFAA CLAIMS.

Ryanair has failed to present evidence supporting key elements of its remaining CFAA claims against Booking.com, requiring judgment as a matter of law for Booking.com.

A. Count IV (18 U.S.C. § 1030(a)(5)(B)-(C)) (Access Without Authorization)

Under Count IV, Ryanair must establish Booking.com’s intentional access of a Ryanair computer without authorization by directing, encouraging, or inducing a third party to do so, and, as a result, recklessly causing Damage, or causing both Damage and Loss. D.I. 442 at 4-5. Ryanair’s evidence does not allow a reasonable jury to find these elements.¹⁰

No “intentional access.” Ryanair has failed to show at trial that Booking.com “intentionally accesse[d]” Ryanair’s system, either directly or through a third-party. 18 U.S.C. § 1030(a)(5)(C). “Intentional access” is a requirement for a violation of this provision, even if done through a third-party. Ryanair’s trial evidence shows no intent by Booking.com to access Ryanair’s computers; to the contrary, it shows, at most, Booking.com’s retention of a vendor and intent to obtain the flight inventory that such vendor has.

Not “without authorization.” Ryanair has failed to show at trial that Booking.com or any of its vendors accessed Ryanair’s site “without authorization” under the Court’s summary judgment order, to mean that “defendants have accessed the password-protected portion of Ryanair’s website, either directly or vicariously.” D.I. 399 at 20. Ryanair has failed to show that Booking.com, or any of its vendors, makes bookings for Booking.com customers by accessing the myRyanair portion of the Ryanair website.

¹⁰ Booking.com preserves its objection to the Court’s ruling regarding what constitutes access “without authorization” on a public website such as Ryanair.com (including myRyanair), but even under the standards set forth in the MSJ Opinion, Booking.com is entitled to judgment.

No “directing, encouraging, or inducing.” As explained above, at most, the evidence shows that Booking.com retained a vendor that obtained flight inventory for Booking.com as a general matter—not with respect to Ryanair in particular, and not in any particular manner. This is not sufficient for vicarious liability under the CFAA.¹¹

No “recklessly causing Damage.” Ryanair’s trial evidence has failed to allow a reasonable jury to conclude that Booking.com either acted “recklessly” or that Booking.com caused “Damage.” “Recklessness” requires that a defendant be aware of a substantial and unjustifiable risk of a fact or circumstance required for the violation (or that the result required for the violation would be caused by its actions) and that the defendant consciously disregarded that risk. D.I. 409-3. Ryanair’s evidence falls far short of this standard.

Damage is a specially defined term by the CFAA, and Ryanair has failed to establish Damage with evidence at trial. *See* 18 U.S.C. § 1030(e)(8) (defining “damage” as “any impairment to the integrity or availability of data, a program, a system, or information”). As explained above with respect to Ryanair’s claims of “loss,” there has been no showing that Ryanair’s systems were impaired by any actions of Booking.com.

No “causing both Damage and Loss.” Ryanair also has not presented evidence showing that Booking.com “caused both Damage and Loss” to Ryanair—for all the reasons discussed above. No reasonable jury could find that Booking.com caused Ryanair technological harm (“damage”) or concrete damage to Ryanair flowing from any such harm (“loss”).

¹¹ Booking.com preserves its objection to the Court’s ruling that vicarious liability is satisfied by a showing of “direct, induce, encourage,” as opposed to an agency relationship or “purposeful direction.” *See* MSJ Op. at 37-38. But Ryanair’s trial evidence has failed to show even that Booking.com “directed, induced, or encouraged” any vendor to violate the CFAA.

B. Count II (18 U.S.C. § 1030(a)(4)) (Fraud)

Under Count II, Ryanair must establish that Booking.com knowingly and with the intent to defraud, directed, encouraged, or induced a third party to access Ryanair's computers without authorization, and by means of such conduct, furthered the intended fraud and obtained something of value for Booking.com. D.I. 442 at 4-5.

In addition to other elements encompassed by Count IV above, Ryanair's fraud claim under 18 U.S.C. § 1030(a)(4) requires Ryanair to show that Booking.com acted "knowingly and with intent to defraud." D.I. 399 at 43-45. An "intent to defraud" under the CFAA requires that a defendant act "willfully and with specific intent to deceive or cheat, usually for the purpose of getting financial gain for himself or causing financial loss to another." *Fidlar Techs. v. LPS Real Est. Data Sols., Inc.*, 810 F.3d 1075, 1079 (7th Cir. 2016); *see* D.I. 399 at 44-45. A showing that a defendant merely engaged in general wrongdoing to obtain something of value is insufficient to allege an intent to defraud. *QVC, Inc. v. Resultly, LLC*, 159 F. Supp. 3d 576, 597-98 (E.D. Pa. 2016); *see also id.* at 581 (notwithstanding the plaintiff's allegation that the defendant had improperly used a web crawling program to crawl the plaintiff's web server, the court found that the plaintiff had "fail[ed] to allege any 'intent to defraud' whatsoever"). Thus, the Court left open in its summary judgment order that Ryanair may be able to prove at trial that Booking.com "access[es] the Ryanair website by dishonest means, that is, by using 'false' contact and payment information." D.I. 399 at 45.¹²

At trial, however, Ryanair did not present *any* evidence that Booking.com acted "willfully and with specific intent to deceive or cheat" Ryanair. *Fidlar Techs.*, 810 F.3d at 1079. To the contrary, the record before the jury at the close of Ryanair's case shows that Booking.com used a

¹² Booking.com preserves its objection to allowing this theory of fraud to proceed to trial. Nonetheless, Ryanair's evidence at trial has failed to meet the standard in the MSJ Opinion.

third-party vendor to make flight bookings on hundreds of airlines, including Ryanair; that Ryanair was paid fully for all those flights; that Ryanair received real, usable email addresses and payment information for Boooking.com flights (not “fake” information); and that, while Booking.com was aware of Ryanair’s dislike of Booking.com’s use of a third-party vendor to obtain Ryanair flights, Booking.com believed that there was nothing wrong with doing so, and, indeed that Ryanair had a long history of bringing meritless lawsuits to bully OTAs. 7/16/24 Trial Tr. at 287-88 (Hurley); *id.* at 495-96 (Guerrero). No reasonable jury can find an intent to defraud on this record.

C. Count V (18 U.S.C. § 1030(b)) (Conspiracy)

Under Count V, Ryanair must establish that Booking.com conspired with third parties to commit a violation of the Computer Fraud and Abuse Act. D.I. 442 at 4-5. The Court’s Summary Judgment Opinion explained that to hold Booking.com liable for a CFAA conspiracy, Ryanair would have to show not only an underlying CFAA violation, but also that Booking.com was part of a “knowing ‘agreement and common activities in furtherance of the unlawful act.’” D.I. 399 at 48 (quoting cases). Additionally, Ryanair must show that Booking.com “joined the agreement or conspiracy knowing of its objective(s) to violate the Computer Fraud and Abuse Act” and “intending to join together with at least one other alleged conspirator to achieve that objective.” D.I. 409-3¹³. It is not enough to prove conspiracy for Ryanair to show that Booking.com had an agreement with a vendor whereby it accessed Ryanair inventory. That is so because conspiracy requires “a unity of purpose” to achieve a common, unlawful objective—here, violation of the CFAA. Ryanair’s evidence before the jury does not allow a reasonable juror to make that conclusion, because Booking.com had no intent or objective to violate the CFAA, let alone a

¹³ This element of a conspiracy was not addressed in the MSJ Opinion and is required for a conspiracy finding. To the extent that the MSJ Order relieved Ryanair from its burden of proving all elements of a CFAA conspiracy, Booking.com preserves its challenge to that framework.

shared one with its vendors. To the contrary, the evidence shows that Booking.com believed there was nothing wrong about getting Ryanair inventory and was given assurances by its vendor, Etraveli, to that effect—a vendor whose contract required it at all times to act in compliance with law. DTX-243. No conspiracy exists on this record.

V. DEFENDANTS ARE ENTITLED TO JUDGMENT AS A MATTER OF LAW BECAUSE RYANAIR HAS FAILED TO ESTABLISH A FACTUAL BASIS FOR THE EXTRATERRITORIAL APPLICATION OF THE CFAA.

Early in this litigation, the Court dismissed Defendants’ pleadings-stage challenge to Ryanair’s CFAA claims based on the presumption against the extraterritorial application of U.S. statutes. *See* D.I. 42 at 14-16 (Court’s December 2021 order denying Defendants Motion to Dismiss (“MTD Order”)); D.I. 17 at 21-26 (Defendants’ MTD); D.I. 26 at 18-24 (Ryanair’s MTD opposition); D.I. 27 at 7-9 (Defendants’ MTD reply).¹⁴ The Court rejected Defendants’ argument that this case involves an impermissible extraterritorial application of the CFAA, determining, under the “first step of the Supreme Court’s framework,” that “Congress has provided a ‘clear, affirmative indication’ that the CFAA applies extraterritorially,” D.I. 42 at 15 (quoting *RJR Nabisco, Inc. v. Eur. Cmty.*, 579 U.S. 325, 339 (2016)), by defining “protected computer” to “explicitly include[] computers located outside the United States,” D.I. 42 at 15 (citing 18 U.S.C. § 1030(e)(2)(B)). The Court further rejected Defendants’ contention that, notwithstanding the statute’s broad definition of “protected computer,” the CFAA cannot be interpreted to apply to conduct “by foreign actors to a foreign website causing foreign harm,” *id.* at 16 (citing D.I. 17 at 21)—*i.e.*, where ‘the alleged perpetrator, the alleged victim, the alleged website, and all alleged

¹⁴ This “presumption serves to avoid the international discord that can result when U.S. law is applied to conduct in foreign countries and reflects the commonsense notion that Congress generally legislates with domestic concerns in mind.” *Abitron Austria GmbH v. Hetronic Int’l, Inc.*, 600 U.S. 412, 417 (2023) (quoting *RJR Nabisco, Inc. v. European Community*, 579 U.S. 325, 335–336 (2016)) (cleaned up).

instrumentalities are located outside of the United States.” D.I. 42 at 15 (quoting D.I. 17 at 24). According to the Court, this interpretive concern—that the CFAA’s definition of “protected computer” would swallow the presumption against extraterritorial application of the statute¹⁵—did not arise in this case because “Ryanair charges that three Delaware companies, along with two foreign companies in the same corporate family, engaged in conduct that violates the CFAA—some of which conduct (e.g., using data obtained by screen scraping) may have occurred in the United States for websites that are accessible in the United States.” D.I. 42 at 15.

Now, however, all Defendants other than Booking.com have been voluntarily dismissed with prejudice from this lawsuit. These voluntarily dismissed defendants included US-based Priceline, KAYAK and Booking Holdings. The sole remaining defendant, Booking.com BV, is a company based in Amsterdam, the Netherlands, and so the case now involves a dispute between two European companies over airfares offered only in Europe, with the relevant computer servers sitting entirely in Europe. Therefore, applying the CFAA in this case would amount to an impermissible extraterritorial application of U.S. law. Accordingly, motion for judgment as a matter of law should be granted to Booking.com.

Since the Court’s MTD Order, the Supreme Court has spoken again about the proper framework for assessing a claim of impermissible extraterritorial application of a U.S. statute, in an analysis that shows why application of the CFAA in this case is improper. In *Abitron Austria*

¹⁵ Defendants argued that to allow the CFAA to “cover[] every computer intrusion in the world” “because the CFAA’s definition of ‘protected computer’ includes computers involved in foreign commerce,” D.I. 27 at 5, “would swallow the presumption against extraterritoriality and transform the United States into the worldwide enforcer against computer hacking,” despite there being “no indication whatsoever that Congress intended such a result.” D.I. 17 at 24. Booking.com preserves its challenge to the Court’s pleadings-stage ruling regarding extraterritoriality, but, as set forth in this motion, judgment as a matter of law is required based on the ultimate facts at trial, which indicate that applying the CFAA here would be an impermissible extraterritorial application.

GmbH v. Hetronic Int'l, Inc., 600 U.S. 412 (2023), the Supreme Court rejected extraterritorial application of key provisions of the Lanham Act. *See id.* at 428. As the Supreme Court explained, “[i]t is a ‘rare statute that clearly evidences extraterritorial effect despite lacking an express statement of extraterritoriality,’” *id.* at 420 (quoting *RJR Nabisco*, 579 U.S. at 340), and that neither “an express statutory reference to ‘foreign commerce,’” nor “a definition of ‘commerce’ that refers to Congress’s authority to regulate foreign commerce” is “enough to rebut the presumption.” *Abitron*, 600 U.S. at 420-21.

Here, the Court’s MTD Order rejecting Defendants’ extraterritoriality challenge hinged the fact that “[t]he CFAA defines the term ‘protected computer’ to include a computer ‘used in or affecting interstate or foreign commerce or communication, including a computer located outside the United States that is used in a manner that affects interstate or foreign commerce or communication of the United States.’” MTD Order at 15 (quoting 18 U.S.C. § 1030(e)(2)(B)). However, under *Abitron* (and precedent cited therein), references to “foreign commerce” and “affects . . . foreign commerce” are insufficient to rebut the presumption against extraterritoriality. And the additional words “computer located outside the United States” cannot mean any computer in the world, regardless of circumstance. Were that the case, there would be no limiting principle and the CFAA—which became law in 1986, years before the rise of the internet—could be applied to any activity involving a computer outside the United States, given that courts have interpreted “protected computer” to mean “effectively all computers with Internet access.” *United States v. Nosal*, 676 F.3d 854, 859 (9th Cir. 2012).

The Court’s MTD Order did not rule out interpreting the CFAA to exclude extraterritorial application “where ‘the alleged perpetrator, the alleged victim, the alleged website, and all alleged instrumentalities are located outside of the United States.’” D.I. 42 at 15 (quoting D.I. 17 at 24).

To the contrary, it concluded only that these were not the facts pled by Ryanair, *see* D.I. 42 at 15. Now, however, Ryanair’s evidence at trial shows that it is seeking only an unauthorized extraterritorial application of the CFAA, as the alleged perpetrator (Booking.com), the alleged victim (Ryanair), the alleged website (Ryanair’s computers), and the alleged instrumentality (Etraveli) are *all* located outside the United States. There are no longer any domestic defendants, and no domestic computer servers allegedly harmed, to tie the case at hand to the United States in even a tangential manner. No reasonable jury could conclude anything other than the following facts: Booking.com is a Dutch company whose asserted conduct occurred abroad; Ryanair is an Irish company whose asserted harm occurred to its computers abroad; and Etraveli is a Swedish company whose asserted conduct occurred abroad. 7/15/24 Trial Tr. at 133; 7/16/24 Trial Tr. at 337, 364 (Hurley); 7/16/24 Trial Tr. at 425 (Guerrero). Indeed, now that all United States-related Defendants have been dismissed from this case, the *only* connection to the United States arguably shown by Ryanair at trial is that “graphics” on Ryanair’s website (which is otherwise located in Ireland) pull from local servers, and thus a U.S. user of Ryanair’s website (on which only intra-European flights are available) may pull “graphics” content from servers located in the United States. 7/15/24 Trial Tr. at 133 (Hurley). But this case is not about any harm to U.S. users of Ryanair’s website who are unable to access graphical content. It is about whether *Ryanair’s* computers in Ireland are harmed by the actions of Booking.com or its vendor Etraveli, both located in Europe. And there has been *zero* evidence at trial showing that any of that harm—or any relevant conduct at all—occurred in the United States. This case therefore presents a situation in which Congress did not authorize extraterritorial application of the CFAA, because the only connection between Ryanair’s case at trial and the United States is that Ryanair’s allegedly affected computers are in “foreign commerce,” which is insufficient to support extraterritorial application.

See Abitron, 600 U.S. at 420 (explaining that “[w]hen applying the presumption, we have repeatedly held that even statutes . . . that expressly refer to “foreign commerce” when defining “commerce” are not extraterritorial (cleaned up)).¹⁶

Because Ryanair has failed to show that the CFAA can apply extraterritorially on the facts presented at trial, it would only be able to establish CFAA liability by showing a “(permissible) domestic . . . application.” *Abitron*, 600 U.S. at 418. Ryanair cannot make such a showing here (and the Court’s MTD Order did not reach that issue), because Ryanair has not shown that “the conduct relevant to the statute’s focus occurred in the United States.” *Id.* (cleaned up). The CFAA’s “focus” is harm to protected computers, and here there has been no evidence of any harm to a Ryanair computer (or any computer) in the United States.

VI. CONCLUSION

For the foregoing reasons, Booking.com respectfully request that the Court grant it judgment as a matter of law as to all of Ryanair’s remaining claims (Counts II, IV, and V).

¹⁶ To the extent the MTD Order interpreted the CFAA to have extraterritorial application in all cases involving a computer outside of the United States connected to the internet—meaning that the CFAA would cover situations involving any computer, any defendant, and any plaintiff, anywhere—such an interpretation of the CFAA is mistaken and contrary to the Supreme Court’s framework for assessing extraterritoriality.

OF COUNSEL:

John H. Hemann
Kathleen Hartnett
Kristine Forderer
Alexander J. Kasner
Jessie Simpson LaGoy
Hannah Pollack
Zoë Helstrom
COOLEY LLP
3 Embarcadero Center St., 20th Fl.
San Francisco, CA 94111
(415) 693-2200
jhemann@cooley.com
khartnett@cooley.com
kforderer@cooley.com
akasner@cooley.com
jsimpsonlagoy@cooley.com
hpollack@cooley.com
zhelstrom@cooley.com

Dated: July 17, 2024

/s/ Jeffrey L. Moyer

Jeffrey L. Moyer (#3309)
Alexandra M. Ewing (#6407)
Richards, Layton & Finger, P.A.
One Rodney Square
920 N. King Street
Wilmington, DE 19801
(302) 651-7700
moyer@rlf.com
ewing@rlf.com

*Attorneys for Defendant/Counterclaim Plaintiff
Booking.com B.V.*